



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/822,242	04/08/2004	Daniel M. Wong	OR03-17301	1781
------------	------------	----------------	------------	------

51067 7590 02/20/2008
ORACLE INTERNATIONAL CORPORATION
c/o PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER

REYES, MARIELA D

ART UNIT	PAPER NUMBER
----------	--------------

2167

MAIL DATE	DELIVERY MODE
-----------	---------------

02/20/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

Response to Amendment

This Office Action has been issued with respect to the amendment received November 23rd, 2007. Claims 1-6, 8-16, 18-26 and 28-30 are pending; Claims 7, 17 and 27 have been cancelled. Applicant's arguments have been carefully and respectfully considered,

Claim Rejections - 35 USC § 101

Claims 11-16 and 18-20 are considered statutory in view of the withdrawal of carrier waves from the definition presented in applicant's specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 5, 6, 8-13, 15, 16, 18-23, 25, 26 and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellison et al (US Patent 6,487,547) in view of Ho (US Patent 6,148,342).

With respect to independent claim 1:

Ellison teaches:

A method for configuring a database, comprising:

Requesting database configuration information from a directory server that stores configuration information for a plurality of database instances; (Column 2 Lines 40-48, discloses a centralized repository that stores the configuration information requested by a database)

In response to the request, receiving the database configuration information from the directory server; (Column 2 Lines 40-48, discloses that the databases configuration information will be communicated by the centralized repository)

Automatically configuring the database with the database configuration information received from the directory server; (Column 2 Lines 40-48, discloses that the database will be configured using the configuration information received from the centralized repository)

Whereby the database server can be installed without manual configuration by a user. (Column 2 Lines 44-48, discloses that the configuring of the database is done by an operation system without any manual configuration by a user)

Ellison does not appear to explicitly disclose:

Receiving a request for resources at the database from a user;

Determining if the user is an enterprise user;

If so, querying the directory server for a user profile associated with the user;

Receiving file user profile from file directory server;

Allocating resources to the user based on parameters specified in the user;

and

The steps of determining if the user is an enterprise user, receiving the user profile, and allocating resources to the user occur within the database.

Ho discloses:

Receiving a request for resources at the database from a user; (Column 2 Lines 52-55, discloses a user requesting information from a database)

Determining if the user is an enterprise user; (Column 4 Lines 3-6, discloses that a user ID is used to identify the user in a look up table to determine the access rights of the user)

If so, querying the directory server for a user profile associated with the user; (Column 4 Lines 11-15, discloses an example in which a doctor's access rights are first identified and then the doctor is allowed to access the information according to his access rights)

Receiving file user profile from file directory server; (Column 4 Lines 11-15, discloses that after a user's access rights are determined then this access rights will be used to allow a user to access the information for which it has privileges)

Allocating resources to the user based on parameters specified in the user; and (Column 4 Lines 3-6, discloses that a user will be assigned user privileges according to a User ID)

The steps of determining if the user is an enterprise user, receiving the user profile, and allocating resources to the user occur within the database. (Column 3 Lines 63-67, discloses that determining a user's access privileges and determining what information he can access is done within an identifier database)

It would be obvious for someone with ordinary skill in the art at the time of the invention to combine the teachings of the cited references to implement **receiving a request for resources at the database from a user; determining if the user is an enterprise user; if so, querying the directory server for a user profile associated with the user; receiving file user profile from file directory server; allocating resources to the user based on parameters specified in the user; and the steps of determining if the user is an enterprise user, receiving the user profile, and allocating resources to the user occur within the database** because this would make accessing the database much more secure by prohibiting access to users who don't have specific privileges.

With respect to claim 2:

Ellison teaches:

The database is structured as a database server, and wherein the database configuration information includes service-related settings for the database server.

(Abstract, discloses that the database is a database server and that the configuration information is related to service settings)

With respect to claim 3:

Ellison teaches:

The database configuration option can include: an audit trail; a security model; a security protocol parameter; a maximum sessions parameter; a database block size;

an optimization mode parameter; and an OLAP features parameter. **(Column 8 Lines 47-61, discloses that the configuration options can be related and include OLAP features parameters)**

With respect to claim 5:

Ellison teaches:

The directory server is Highly Available (HA). **(Column 2 Lines 51-55, discloses that the server will be available through the Internet, therefore making the communication with it Highly Available)**

With respect to claim 6:

Ellison teaches:

Caching a local copy of the configuration information to facilitate configuration of the database when the database cannot connect to the directory server. (Column 5 Lines 3-17, discloses that the data could be locally cached for it to be accessed)

With respect to claim 8:

Ellison does not appear to explicitly disclose that a **user profile can include: a CPU quota for the user; a disk quota for the user; a scheduling priority for the user; and a read/write/execute permission for the user.**

Ho teaches that a **user profile can include: a CPU quota for the user; a disk quota for the user; a scheduling priority for the user; and a read/write/execute permission for the user.** (Column 4 Lines 13-15, discloses that the user access level includes the type of actions the user can do in the database as review or add information)

With respect to claim 9:

Ellison does not appear to explicitly disclose that **the database configuration information can define a Security Admin (SA) role for the database.**

Ho teaches that **the database configuration information can define a Security Admin (SA) role for the database.** (Column 4 Lines 13-15, discloses that the user profile will include information about priority and user rights in the database, therefore defining administrative and normal user roles)

With respect to claim 10:

Ellison teaches:

The database server periodically queries the directory server for updated database configuration information for the database. (Abstract, discloses that the database queries the repository to see if changes in the environment have taken place)

With respect to independent claim 11:

Ellison teaches:

A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for configuring a database, the method comprising:

Requesting database configuration information from a directory server that stores configuration information for a plurality of database instances; (Column 2 Lines 40-48, discloses a centralized repository that stores the configuration information requested by a database)

In response to the request, receiving the database configuration information from the directory server; (Column 2 Lines 40-48, discloses that the databases configuration information will be communicated by the centralized repository)

Automatically configuring the database with the database configuration information received from the directory server; (Column 2 Lines 40-48, discloses that the database will be configured using the configuration information received from the centralized repository)

Whereby the database server can be installed without manual configuration by a user. (Column 2 Lines 44-48, discloses that the configuring of the database is done by an operation system without any manual configuration by a user)

Ellison does not appear to explicitly disclose:

Receiving a request for resources at the database from a user;

Determining if the user is an enterprise user;

If so, querying the directory server for a user profile associated with the user;

Receiving file user profile from file directory server;

Allocating resources to the user based on parameters specified in the user;

and

The steps of determining if the user is an enterprise user, receiving the user profile, and allocating resources to the user occur within the database.

Ho discloses:

Receiving a request for resources at the database from a user; (Column 2 Lines 52-55, discloses a user requesting information from a database)

Determining if the user is an enterprise user; (Column 4 Lines 3-6, discloses that a user ID is used to identify the user in a look up table to determine the access rights of the user)

If so, querying the directory server for a user profile associated with the user; (Column 4 Lines 11-15, discloses an example in which a doctor's access rights are first identified and then the doctor is allowed to access the information according to his access rights)

Receiving file user profile from file directory server; (Column 4 Lines 11-15, discloses that after a user's access rights are determined then this access rights will be used to allow a user to access the information for which it has privileges)

Allocating resources to the user based on parameters specified in the user;
and (Column 4 Lines 3-6, discloses that a user will be assigned user privileges according to a User ID)

The steps of determining if the user is an enterprise user, receiving the user profile, and allocating resources to the user occur within the database.

(Column 3 Lines 63-67, discloses that determining a user's access privileges and determining what information he can access is done within an identifier database)

It would be obvious for someone with ordinary skill in the art at the time of the invention to combine the teachings of the cited references to implement **receiving a request for resources at the database from a user; determining if the user is an enterprise user; if so, querying the directory server for a user profile associated with the user; receiving file user profile from file directory server; allocating resources to the user based on parameters specified in the user; and the steps of determining if the user is an enterprise user, receiving the user profile, and allocating resources to the user occur within the database** because this would make accessing the database much more secure by prohibiting access to users who don't have specific privileges.

With respect to claim 12:

Ellison teaches:

The database is structured as a database server, and wherein the database configuration information includes service-related settings for the database server. (Abstract, discloses that the database is a database server and that the configuration information is related to service settings)

With respect to claim 13:

Ellison teaches:

The database configuration option can include: an audit trail; a security model; a security protocol parameter; a maximum sessions parameter; a database block size; an optimization mode parameter; and an OLAP features parameter. (Column 8 Lines 47-61, discloses that the configuration options can be related and include OLAP features parameters)

With respect to claim 15:

Ellison teaches:

The directory server is Highly Available (HA). (Column 2 Lines 51-55, discloses that the server will be available through the Internet, therefore making the communication with it Highly Available)

With respect to claim 16:

Ellison teaches:

The method further comprises caching a local copy of the configuration. (Column 5 Lines 3-17, discloses that the data could be locally cached for it to be accessed)

With respect to claim 18:

Ellison does not appear to explicitly disclose that a **user profile can include: a CPU quota for the user; a disk quota for the user; a scheduling priority for the user; and a read/write/execute permission for the user.**

Ho teaches that a **user profile can include: a CPU quota for the user; a disk quota for the user; a scheduling priority for the user; and a read/write/execute permission for the user.** (Column 4 Lines 13-15, discloses that the user access level includes the type of actions the user can do in the database as review or add information)

With respect to claim 19:

Ellison does not appear to explicitly disclose that **the database configuration information can define a Security Admin (SA) role for the database.**

Ho teaches that **the database configuration information can define a Security Admin (SA) role for the database.** (Column 4 Lines 13-15, discloses that the user profile will include information about priority and user rights in the database, therefore defining administrative and normal user roles)

With respect to claim 20:

Ellison teaches:

The database server periodically queries the directory server for updated database configuration information for the database. (Abstract, discloses that the database queries the repository to see if changes in the environment have taken place)

With respect to independent claim 21:

An apparatus for configuring a database, comprising:

A request mechanism configured to request database configuration information from a directory server that stores configuration information for a plurality of database instances; (Column 2 Lines 40-48, discloses a centralized repository that stores the configuration information requested by a database)

A receiving mechanism configured to receive the database configuration information from the directory server in response to the request; (Column 2 Lines 40-48, discloses that the databases configuration information will be communicated by the centralized repository)

A configuration mechanism configured to automatically configure the database with the database configuration information received from the directory server; (Column 2 Lines 40-48, discloses that the database will be configured using the configuration information received from the centralized repository)

Ellison does not appear to explicitly disclose:

A second receiving mechanism configured to receive a request for resources at the database from a user;

A determination mechanism configured to determine if the user is an enterprise user;

A querying mechanism configured to query the directory, server for a user profile associated with the user if the user is an enterprise user;

A profile mechanism configured to receive the user profile from the directory server;

An allocation mechanism configured to allocate resources to the user based on parameters specified in the user profile; and

The determination mechanism, the querying mechanism, the profile mechanism, and the allocation mechanism are within the database.

Ho discloses:

A second receiving mechanism configured to receive a request for resources at the database from a user; (Column 2 Lines 52-55, discloses a user requesting information from a database)

A determination mechanism configured to determine if the user is an enterprise user; (Column 4 Lines 3-6, discloses that a user ID is used to identify the user in a look up table to determine the access rights of the user)

A querying mechanism configured to query the directory, server for a user profile associated with the user if the user is an enterprise user; (Column 4 Lines 11-15, discloses an example in which a doctor's access rights are first identified and then the doctor is allowed to access the information according to his access rights)

A profile mechanism configured to receive the user profile from the directory server; (Column 4 Lines 11-15, discloses that after a user's access rights are determined then this access rights will be used to allow a user to access the information for which it has privileges)

An allocation mechanism configured to allocate resources to the user based on parameters specified in the user profile; and (Column 4 Lines 3-6, discloses that a user will be assigned user privileges according to a User ID)

The determination mechanism, the querying mechanism, the profile mechanism, and the allocation mechanism are within the database. (Column 3 Lines 63-67, discloses that determining a user's access privileges and determining what information he can access is done within an identifier database)

It would be obvious for someone with ordinary skill in the art at the time of the invention to combine the teachings of the cited references to implement **a second receiving mechanism configured to receive a request for resources at the database from a user; a determination mechanism configured to determine if the user is an enterprise user; a querying mechanism configured to query the directory, server for a user profile associated with the user if the user is an enterprise user; a profile mechanism configured to receive the user profile from the directory server; an allocation mechanism configured to allocate resources to the user based on parameters specified in the user profile; and the determination mechanism, the querying mechanism, the profile mechanism, and the allocation mechanism are within the database** because this would make accessing the database much more secure by prohibiting access to users who don't have specific privileges.

With respect to claim 22:

Ellison teaches:

The database is structured as a database server, and wherein the database configuration information includes service-related settings for the database server. (Abstract, discloses that the database is a database server and that the configuration information is related to service settings)

With respect to claim 23:

Ellison teaches:

The database configuration option can include: an audit trail; a security model; a security protocol parameter; a maximum sessions parameter; a database block size; an optimization mode parameter; and an OLAP features parameter. **(Column 8 Lines 47-61, discloses that the configuration options can be related and include OLAP features parameters)**

With respect to claim 25:

Ellison teaches:

The directory server is Highly Available (HA). (Column 2 Lines 51-55, discloses that the server will be available through the Internet, therefore making the communication with it Highly Available)

With respect to claim 26:

Ellison teaches:

A caching mechanism configured to cache a local copy of the configuration information to facilitate configuration of the database when the database cannot connect to the directory server. (Column 5 Lines 3-17, discloses that the data could be locally cached for it to be accessed)

With respect to claim 28:

Ellison does not appear to explicitly disclose that **a user profile can include: a CPU quota for the user; a disk quota for the user; a scheduling priority for the user; and a read/write/execute permission for the user.**

Ho teaches that **a user profile can include: a CPU quota for the user; a disk quota for the user; a scheduling priority for the user; and a read/write/execute permission for the user.** (Column 4 Lines 13-15, discloses that the user access level includes the type of actions the user can do in the database as review or add information)

With respect to claim 29:

Ellison does not appear to explicitly disclose that **the database configuration information can define a Security Admin (SA) role for the database.**

Ho teaches that **the database configuration information can define a Security Admin (SA) role for the database.** (Column 4 Lines 13-15, discloses that the user profile will include information about priority and user rights in the database, therefore defining administrative and normal user roles)

With respect to claim 30:

Ellison teaches:

The database server periodically queries the directory server for updated database configuration information for the database. (Abstract, discloses that the database queries the repository to see if changes in the environment have taken place)

Claims 4, 14 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellison et al (US Patent 6,487,547) in view of Ho (US Patent 6,148,342) and Nilsen et al (US Patent 5,606,693).

With respect to claim 4:

The above discussed combination of Ellison and Ho does not appear to explicitly disclose that **the configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services.**

Nilsen teaches that **the configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services.** (Abstract, discloses a distributed database application on which the configuration information provided to the database server includes access information, this would allow for better control of the information stored and accessed by the database therefore making the transfer of the data much more secure.

It would be obvious for someone with ordinary skill in the art at the time of the invention to combine the teachings of the cited references to implement that **the configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services** because this allows for better control of the information stored and accessed by the database therefore making the transfer of the data much more secure. (As Seen in Nilsen Column 1 Lines 16-45)

With respect to claim 14:

The above discussed combination of Ellison and Ho does not appear to explicitly disclose that **the configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services.**

Nilsen teaches that **the configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services.** (Abstract, discloses a distributed database application on which the configuration information provided to the database server includes access information, this would allow for better control of the information stored and accessed by the database therefore making the transfer of the data much more secure.

It would be obvious for someone with ordinary skill in the art at the time of the invention to combine the teachings of the cited references to implement that **the**

configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services because this allows for better control of the information stored and accessed by the database therefore making the transfer of the data much more secure. (As Seen in Nilsen Column 1 Lines 16-45)

With respect to claim 24:

The above discussed combination of Ellison and Ho does not appear to explicitly disclose that **the configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services.**

Nilsen teaches that **the configuration information can include an Access Control List (ACL), wherein the ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services.** (Abstract, discloses a distributed database application on which the configuration information provided to the database server includes access information, this would allow for better control of the information stored and accessed by the database therefore making the transfer of the data much more secure.

It would be obvious for someone with ordinary skill in the art at the time of the invention to combine the teachings of the cited references to implement that **the configuration information can include an Access Control List (ACL), wherein the**

ACL lists objects and services available on the database server and which hosts have permissions to use the objects and the services because this allows for better control of the information stored and accessed by the database therefore making the transfer of the data much more secure. (As Seen in Nilsen Column 1 Lines 16-45)

Response to Arguments

Claim Rejections 35 USC 103

With respect to claim 1:

Applicant argues that **“Ho fails to teach determining if the user is an enterprise user because Ho teaches away from the use of enterprise users in favor of local subnetwork administrators”** Examiner respectfully disagrees.

Applicant's specification fails to address the fact that an enterprise user has a unique identity across an enterprise in fact it doesn't define an enterprise user, rather it explains that an enterprise user will be associated with a user profile (Ho's user access rights) that governs the allocated resources, CPU quota for the user, etc. (specification Paragraph [011]-[012]). Ho (Column 4 Lines 3-6) discloses using a user ID to access an approved level of access to certain information (user profile).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mariela D. Reyes whose telephone number is (571) 270-1006. The examiner can normally be reached on M - F 7:30- 5:00 East time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on (571) 272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Application/Control Number:
10/822,242
Art Unit: 2167

Page 23

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MR feb. 04, 08
MR

DL



DEBBIE LE
PRIMARY EXAMINER

2/13/08